SSFN – a SCION ISD in Switzerland
Secure Swiss Finance Network SCION use case

Fritz Steinmann <Fritz.Steinmann@six-group.com>

06/11/2023
SIX – Who we are

SIX operates the Swiss Financial Infrastructure:

- Swiss Stock Exchange (Listing & Trading)
- Financial Information (Reference & Market Data, Indices)
- Securities Services (Central Security Depository, Central Counterparty, Clearing & Settlement)
- Banking Services (Billing & Payment Services, Debit & Mobile Services, ATM Services)

- Interbank services are provided by a private network operated by commercial telco providers
- SIX maintains connections to other banks pan-Europe and in other markets globally
Business and Technical Requirements for a new Interbank Network

- **Trends and Challenges**
  - Real-Time systems such as the Swiss payments system and other critical infrastructures form the strong core for the financial system and must have strongest possible protection
  - Increasing reliance on public networks – the Internet – for communications between financial institutions, bank branches and infrastructures
  - Vulnerability of data in transport is a risk (e.g., due to denial of service or man in the middle attacks)
  - Current solutions to address risks are inflexible and costly

- **Requirements for a new Interbank Network**
  - A secure and resilient communication network for payments and other critical infrastructures
  - Protection against cyber risks: enforceable governance and boundaries
  - Trust in the network – know the location / path of data in transit
  - Flexible communication between participants: any-to-any architecture instead of (virtual) point-to-point connections
  - Delivered by the financial community and telecom providers – no change in business model
SSFN – A Secure and Resilient Communication Network for Interbank traffic

**Today**
Centralized «Hub and Spoke» architecture

**Vision**
Community-based, «any-to-any», Internet-like architecture
Why SCION?

- Before starting, a thorough analysis was started
  - Comparison between different new Internet technologies was done
  - Alternatively, replacing MPLS by another MPLS network was considered
  - SD-WAN was briefly discussed, but is not suited for a multi-provider, multi-product, multi-customer market
- SCION promised to meet the requirements
- SCION had already achieved a high level of maturity in productive use (Swiss National Bank, Swiss Government)
- There was already a close collaboration between SIX and ETH, where SCION was originally researched and developed
What is different in using SCION compared to other technologies?

- SCION allows for local, user-centric, enforceable governance
- Governance can be split from actual operations; the governance parties don’t need to be identical to those who operate the network
- ISD concept allows for complete isolation of trust
- Multiple operations models can be implemented, it allows for various business models
The Governance of SSFN Defines the Rules & Regulations of SSFN – Service Providers Must Qualify

Basic characteristic of SSFN
Regulated interaction between users and service providers (with rules defined by the governance and influenceable by users and service providers), but decentralized like the Internet.

Governance SSFN
Voting members SSFN (SIX, SNB, SWITCH)
Responsible for SSFNs rules and a functioning Trust Root Configuration (TRC)

SSFN Service provider
(Anapaya, service providers SIX, Sunrise, Swisscom, SWITCH, SIX)
Providing the necessary services for the data exchange based on the SCION protocol and the SSFN rulebook

SSFN User
(SIX customers)
Purchase of services from approved SSFN service providers

Run/Use SSFN

How to Be Part of SSFN?
Is accepted as service provider for SSFN, following a transparent onboarding process and contractually confirming to continuously adhere to requirements criteria

Is qualified by using an eligible service from a SIX entity (e.g. SIC) offered via SSFN

1| Service providers can also offer SCION-related services for other ISDs
TRC Creation and Maintenance

- From research perspective, TRC creation and life cycle is well established and well documented (see SCION Control-Plane PKI draft RFC, [https://datatracker.ietf.org/doc/draft-dekater-scion-pki/](https://datatracker.ietf.org/doc/draft-dekater-scion-pki/))
- In practice, key and TRC creation ceremonies must be designed according to ISD requirements
- In a multi-party governed ISD virtual TRC ceremonies have proved to be effective and viable
- Elements in the TRC:
  - ISD ID
  - Purpose
  - Core and authoritative participants (ASes)
  - Validity period
  - Voting Quorum
  - Certificates (CA root, regular and sensitive voting)
  - Some other parameters
TRC Creation and Maintenance

**ISD ID**

**Purpose / Description**

Voting Quorum

Core and authoritative participants (ASes)

Certificates (CA root, regular and sensitive voting)

Validity period
TRC Creation and Maintenance

- The process is basically to:
  - Collect and verify required material (CA root certificates, Sensitive and Regular Voting Certificates)
  - Agree on required parameters (as indicated above)
  - Generate payload (object container)
  - Sign by authoritative parties, verify signatures and content
  - Combine signatures and create final TRC container

```
anapaya@trc-hoster:/$> trc payload --predecessor ISD70-B1-S2.trc --out ISD70-B1-S3.pld.der --template ISD70-B1-S3.toml
Generating payload for TRC update.
required signatures:
  - type: vote
    common name: SIX Regular Voting Certificate
    serial number: 37 F4 66 80 3D 1F E3 6F 77 CE 4C 42 73 D1 56 C3 0F DA D1 CD
  - type: vote
    common name: SNB Regular Voting Certificate
    serial number: 37 92 22 59 3F 56 9E 78 3B A9 4A 63 9A 76 FA DC 01 1A 40 8E
  - type: vote
    common name: SWITCH Regular Voting Certificate
    serial number: 22 A8 4F 13 12 EA 3B 55 8C S1 F5 47 3A D9 F3 E9 7E 23 D4 C6
Successfully created payload at ISD70-B1-S3.pld.der
```
SSFN ISD TRC has been first created in November 2021.

Validity period was set to 395 days.

It was renewed successfully in 2022 and 2023.

Dissemination in the SSFN ISD is seamless.

```
serial_number: 7A 99 D3 EB 1A 31 BE 88 2C 1B 2A 14 C8 16 F3 C4 AA B1 7B DA
validity:
  not_before: 2021-11-01T00:00:00Z
  not_after: 2026-11-01T00:00:00Z
index: 5
- type: regular-voting
  common_name: SWITCH Regular Voting Certificate
  isd_as: 70-559
serial_number: 22 A8 4F 13 12 EA 38 55 8C 51 F5 47 3A D9 F3 E9 7E 23 D4 C6
validity:
  not_before: 2021-11-01T00:00:00Z
  not_after: 2026-11-01T00:00:00Z
index: 6
- type: cp-root
  common_name: SWITCH SSFN CP Root CA
  isd_as: 70-559
serial_number: 6C 97 5E 08 71 77 30 61 47 B0 73 51 3A B2 F6 B8 S1 26 C4 B5
validity:
  not_before: 2021-11-01T00:00:00Z
  not_after: 2032-11-01T00:00:00Z
index: 7
```

```
anapaya@trc-hoster:/opt/trc-ceremony-20231026$ sha256sum ISO70-B1-S3.pld.der
ba171950d48750a345b21345bb8738d844a092b8c1bf09d433f1f578aa ISO70-B1-S3.pld.der

anapaya@trc-hoster:/opt/trc-ceremony-20231026$ mv switch/ISO-B1-S3.regular.vote.der switch/ISO70-B1-S3.regular.vote.trc

anapaya@trc-hoster:/opt/trc-ceremony-20231026$ sha256sum snb/ISO70-B1-S3.regular.vote.trc
3dcf27a4e19f4ecbf1815db5e8f86ab282d175fadb51e0b59aca2a24133fa snb/ISO70-B1-S3.regular.vote.trc

anapaya@trc-hoster:/opt/trc-ceremony-20231026$ sha256sum switch/ISO70-B1-S3.regular.vote.trc
59d1a3c52595b758d34a7a1a83893159e21e8dc2f67be771c4e1a18ca5369a switch/ISO70-B1-S3.regular.vote.trc

anapaya@trc-hoster:/opt/trc-ceremony-20231026$ sha256sum six/ISO70-B1-S3.regular.vote.trc
b0370fcd4bb943bc346dc8059c5294a2716c71899c336e3f91e9ef47e1120c9 six/ISO70-B1-S3.regular.vote.trc

anapaya@trc-hoster:/opt/trc-ceremony-20231026$ scion-pkt trc combine -p ISO70-B1-S3.pld.der \\
> six/ISO70-B1-S3.regular.vote.trc
> snb/ISO70-B1-S3.regular.vote.trc
> switch/ISO70-B1-S3.regular.vote.trc
> o ISO70-B1-S3.trc

Successfully combined TRC at ISO70-B1-S3.trc
anapaya@trc-hoster:/opt/trc-ceremony-20231026$ scion-pkt trc verify --anchor ISO70-B1-S2.trc ISO70-B1-S3.trc

Verified TRC successfully: ISO70-B1-S3.trc
anapaya@trc-hoster:/opt/trc-ceremony-20231026$
Challenges / How could IETF help?

- Lack of adoption
  - Although SSFN is a completely functional and flawlessly operating network, it is but a lighthouse implementation
  - None of the bigger network software companies picked up SCION implementation so far
  - None of the bigger ISP’s showing interest in deploying SCION so far
- Lack of operational authorities (e.g., numbering) / global governance → addressed by SCION Association
- Lack of standardization → can be addressed at IETF
- There will be more work at IETF needed
  - Continuing work on Internet drafts towards RFC’s
  - Aligning with other work
  - Exploring more options